6-2012

Employee surveillance and the modern workplace

Marko PITESA
Singapore Management University, mpitesa@smu.edu.sg

Employee Surveillance and the Modern Workplace

Chapter Overview

Employee surveillance is rapidly becoming widespread in the modern workplace. The rise of information technologies is enabling the development of unprecedented methods of surveillance and employees as well as employers are now facing a need for a reassessment of the system of moral relations this phenomenon entails. This chapter provides an overview of the most widespread workplace surveillance methods and tries to identify the stakeholders and analyse the relations between them. Finally, the key findings of this ethical assessment are pointed out and guidelines for a morally responsible approach to workplace surveillance are proposed. The level of the analysis, in terms of the classification presented in Chapter two, is primarily the relation between a single company and its stakeholders. However, many of these concerns relate to fundamental societal principles and as such can only be fully appreciated if one takes into account the rootedness of business in overall societal dynamics.

Modern Employee Surveillance

Jeremy Bentham once envisioned a method of controlling people by way of maintaining nothing more than a constant possibility of surveillance. The observing entity should not be visible to the observed subjects, which is to say that there is no telling when the surveillance is actually taking place. The very awareness of the fact that one *might* be watched at any given time brings the observed subject into compliance as the only definite way to avoid risk. In effect, this psychological game makes the observed subject internalize the intentions of the observing entity because any speculations as to the exact moment of observation are rendered no longer sensible. This model of surveillance thus ultimately provides the observer with an elegant and effective way of controlling the mind of the observed.

Although Bentham's system of control was designed to control prisoners and not employees, the psychological effects Bentham described and the ones at play in the modern workplace may at times seem surprisingly similar. Employee surveillance is becoming increasingly widespread and comprehensive. An recent survey found that 66% of the companies surveyed monitor internet connections, 45% track content, keystrokes and time spent at the keyboard and 43% store and review computer files. Monitoring employee network activity even extended to the blogosphere and social networking sites. Furthermore, 45% of the companies monitor time spent on the telephone and record numbers called, up from only 9% in 2001, and 16% actually tap and record phone conversations, a 66% increase from 2001. Almost half of the companies now use video monitoring versus one third in 2001. Employers have even been adopting the latest technologies such as Assisted Global Positioning and Global Positioning System to track employee vehicles, cell phones and even ID/Smartcards.

Employee surveillance is greatly facilitated by the advancement of information technologies. The majority of the companies monitoring employees now rely on various IT solutions, making this once burdensome and expensive activity cheap and effective. In fact, most of the modern surveillance methods, and particularly those concerned with computer activity, do not include any human involvement. Disciplining resulting from network surveillance activities is virtually a commonplace. More than 60% of companies have disciplined employees for violations of network policies, 25% have fired employees for inappropriate use of e-mail and nearly one third have fired employees for misusing the Internet. The leading violations include access to pornography, online chat, gaming, investing, or shopping at work.[1] [2] Most of this was not even possible, let alone sanctioned, just twenty years ago.

---

[1] AMA/ePolicy Institute Research. 2008. 2007 Electronic Monitoring & Surveillance Survey. [internet] Available at:

Airline reservation agents, using telephonic headsets to perform their job, widely felt the impact of new surveillance technologies. The length and content of all their telephone calls is usually electronically monitored, and maximum time allowed between calls, sometimes set as low as 10 seconds, can be automatically regulated by computer. In addition, computers are even used to assess how polite agents are, using such criteria as the number of times they mention the customer's name. Evidently, the use of modern, technology-based surveillance is unprecedented in the history of employer-employee relationship and as such challenges much of what has been established as appropriate, normal and expected in the domain of employer oversight. Technology is used to monitor personnel in ways never before imagined, urging us to rethink the moral concerns surrounding the phenomenon of employee surveillance.

To express it using the taxonomy presented in chapter 2, the aim of any ethical analysis dealing with the issue of employee surveillance should be both positive as well as normative. It is important to adequately appreciate the drastic changes taking place in the domain of employee surveillance, to take stock of the concerns of the parties involved and to descriptively situate the moral challenges arising from the question of employee surveillance today within the existing body of ethics and legal regulation. However, one is also urged to go further and to try to offer a way to interpret these changes normatively, to offer a direction arising from the account of the situation and against the backdrop of moral concerns and established principles. Eschewing normative discussion lest one be exposed to academic criticism seems irresponsible when the issue in question impacts employees all around the

---

http://www.amanet.org/training/seminars/2007-Electronic-Monitoring-and-Surveillance-Survey-41.aspx [Accessed 17 November 2009].

[2] Similar figures are documented around the world, see:
Schulman, A. (2001). The extent of systematic monitoring of employee e-mail and Internet use. Privacy Foundation. [internet] Available at: http://www.sonic.net/~undoc/extent.htm [Accessed 17 November 2009].

world and when the lagging legal response is in need of an adequate account of moral complexity at play.

Analysis of Key Stakeholders

How is this tremendous growth in workplace surveillance justified? Employers are primarily concerned with competitiveness, job efficiency and profitability. Few would deny corporations the right to select the best possible employee for the job in a competitive economy, which at the very least includes some degree of insight into who a given candidate is and what he or she is capable of. Such insight is impossible without **background checks**, which often include extensive job application informational requirements, credit reports, and the like. On the other hand, the concerns in relation to efficiency, performance and productivity also form the basis of the need for **on the job employee surveillance**. Corporations have the right to manage the workplace toward profit and it is not unreasonable on their part to ask whether their employees are actually contributing to that goal. Being able to verify that an employee is doing the job he or she is paid for arguably constitutes a fundamental part of any employment contract. In addition, employees are increasingly becoming the most significant cost driver, as the increased complexity of their duties calls for ever higher levels of employee education, on the job training, and other factors that increase the necessary remuneration. Finally, employees are more and more becoming not just the dominant cost, but even more importantly the main source of profitability and innovation. In the knowledge economy, business success is less dependent on equipment or capital, both of which are becoming easily-available, and employees make the decisive difference between winners and losers. How could then corporations be denied the right to do everything possible to influence and control this most important factor of modern business?

A number of other arguments can be put forward in defence of employee surveillance. Firstly, surveillance could be necessary in order to make a fair differentiation between

employees - hard-working employees should be compensated relatively more than their less effective coworkers. But if the employer is denied sufficient insight into employee activities, how is this differentiation to be made? Some degree of surveillance just might be necessary to counter misrepresentations regarding performance, hours, and expenses, which morally harm the employees (by making a fair assessment of employee effectiveness harder) as much as they harm the employer. Another argument for surveillance is that companies are understandably cautious about their trade secrets, and in certain situations surveillance might be necessary to protect against leaks. The same logic applies to the protection of client data (from sensitive medical information to credit card details) which might be at risk if adequate protection measures, potentially including some surveillance, are not in place. Another justification for surveillance stems from legislation – employers are increasingly held responsible for the actions of their employees. It is therefore reasonable that employers should seek to gather as much information on their employees as possible in order to protect themselves from vicarious liability or negligent hiring charges. Finally, employee theft, sometimes speculated to be costing businesses billions of euros per year, is another potential justification for the implementation of employee surveillance.

Are these many arguments sufficient to justify workplace surveillance? This is the point at which one must look at how well these principles, rights and concerns apply to particular jobs. Many jobs are compensated upon specific performance, so what rationale could one give for surveillance in such instances? Evidently, the nature of the job makes an importance difference. In some cases, assessing actual performance of a certain activity might be almost impossible without surveillance. Aforementioned airline reservation is one such profession. If the agents weren't under surveillance, what would stop them from not taking any calls? But does this automatically entitle employers to subject these employees to permanent surveillance? Obviously, analysing the nature of the job does not tell us *how much*

surveillance is appropriate. In order to find that balance, the moral stakes of both parties involved, employers and employees, have to be contrasted and appreciated in a broader context of societal dynamics and fundamental ethical principles. We thus proceed to outline the principal concerns of employees in relation to workplace surveillance.

The central concern for employees in the matter of surveillance is the right to privacy. There have been numerous attempts to lay firm foundations of the right to privacy philosophically. Privacy rights can be perceived as necessary to protect such values as self-determination, arguably essential to the individual's status as a person. This line of reasoning treats privacy as serving to establish a boundary between individuals, thus defining one's individuality. However, departing from such very general observations, there is little consensus in relation to the nature, extent, and importance of privacy. Some countries do not recognize a legal right to privacy, while others consider it a fundamental human right. Legal regulation of workplace surveillance varies correspondingly, from the very poor protection of employee privacy in the US and many third-world countries, to more ambitious regulation in the EU, New Zealand and Australia. Philosophical literature views the right to privacy primarily as the right to control information about oneself. But it is obvious that this right or privilege is considered subordinated to numerous other rights. For example, the state can issue an authorization for surveillance if more important interests, such as public safety, are at stake. In addition, most would argue that even in some everyday situations the right to privacy can be considered to be suspended or reduced. For example, public officials' right to privacy is sometimes argued to be reduced because of the public nature of their office and the public interests vested in them. It is also contended that employees renounce their right to privacy when they enter an employment contract to a degree to which the right to privacy might conflict with their contractual obligations. But this still doesn't help much in determining a just boundary of workplace surveillance. For example, inner feelings and desires of a

candidate are certainly relevant to someone trying to assess a candidate's fitness for a position. The candidate may be secretly unenthusiastic about the job he or she is applying for, and the company could be considered to be justified in presuming this could affect the candidate's potential performance. But we are still not comfortable with the idea that Wal-Mart is somehow *entitled* to learn about our inner feelings and desires during a preliminary job interview.

Apart from the right to privacy, other concerns might go against the argument for an extensive surveillance in the workplace. It is easily imaginable how surveillance might create a suspicious and hostile environment, harming work morale and productivity. Employee health may be impacted as well – one study found that employees under surveillance suffer more often from depression and anxiety. In addition, they exhibit more often chronic fatigue, strain injuries, and even neck problems.[3] Finally, the fact that workers are pressured to spend increased hours at work means that it may often be necessary to conduct some pressing personal business at the office. This fact must be respected and taken into account when designing surveillance mechanisms. There is a strong sense that intimate matters, such as medical reports or family issues, whether dealt with by employees from the workplace or not, should remain private.

Employee surveillance, thus, includes two principal stakeholders. On the one hand, employers have the right to verify that the employment contract is being respected by the employee, but they also face numerous other concerns which might call for some form of surveillance. On the other hand, employees are deeply personally affected by how their workplace is organized, and being under surveillance can be not only annoying but deeply frustrating, debilitating and unjust.

---

[3]Kolb, R. W. Ed., 2008. Encyclopedia of Business Ethics and Society, Volume 5. Thousand Oaks, CA.: Sage Publications. p. 2325

We continue by an overview of the most common modern workplace surveillance methods and an outline of how the conflict between the interests of employers and employees unfolds in these specific circumstances.

Specific Instances and Ethical Concerns

Employee monitoring often begins even before the hiring decision. **Pre-employment testing** now routinely includes such techniques as background checks, tests designed to expose candidate's personality, and inquiries into the nature of candidate's off-work activities, for example the possible use of illegal substances. **Credit reports** are now widely used to learn about financial situation and past financial developments of job candidates. An argument for obtaining a credit report may be that someone heavily indebted is more likely to have weak financial abilities or that that person may be more likely to embezzle money if tempted. But one might have a bad credit report because of circumstances out of that person's control, for example exuberant medical expenses of a family member. Is it then fair to discriminate based on this criterion? In addition, even if someone actually is heavily in debt, is it really ever fair to even presume that this person is more likely to embezzle money? **Driving records** of prospective employees are also frequently checked. It is typical for companies to regularly check an employee's driving record if he or she is performing a job where driving is extensively required, for example delivery or courier services. Arguably, the employer bears the moral burden of insuring that the employee's driving ability is not exposing the public to risk. Similar argument can be put forward in relation to **criminal record checks**. The legal treatment of criminal record checks is usually such that the employer may deny employment to a candidate based on a previous conviction, as long as the felony in question is reasonably related to the job duties. Denying a bank job to a convicted bank robber seems defensible, whereas denying employment because of past arrests (in cases in which conviction did not ensue) or a past drug treatment is more likely to be considered

unjust, and even illegal in some countries. The central argument for performing such checks is the one of safety. Employer can be argued to bear a moral responsibility to scrutinize employees' criminal backgrounds so as to ensure the safety of the people this prospective employee will be in contact with, e.g. co-workers, customers, etc. Finally, the employer, at least in some countries, can reduce the risk of potential litigation by doing so, which arguably presents an incentive arising from legal practice.

But how far are we prepared to allow employers to go in selection based on such screening techniques? The judicial system is obligated to presume innocence regardless of previous misdeeds as a result of strong underpinning societal values. Not discriminating on the grounds of past deeds is an important part of modern notion of fairness and, consequentially, our judicial system, not merely punitory but corrective. We deem second chances important and fair, and why shouldn't we? Human beings are fallible but we still feel that we shouldn't be made prisoners of our past wrongdoings as there is always hope for change. Are corporations not supposed adhere to the same principles?

Drug testing, increasingly widespread among modern corporations, raises similar questions, but also adds some new dilemmas. Several major retail companies, including Home Depot, Ikea, and Wal-Mart, have extensive drug-testing regimes for both prospective and present employees. Many stores even leverage their "drug-free workplace" principles as a marketing tactic. The argument for this practice is simple – work efficiency is adversely affected by employees' substance abuse, and safety of the workplace can be affected as well. The problem with this argument, however, is that drug testing, as it is carried out today, might not be a proper way to test for on the job sobriety in the first place. An employee might be conscientious and always sober on the job, but experimenting with illegal substances in his or her own time. Modern drug testing techniques are unable to make this difference. We are inclined to concede that whether employees are sober on the job is of employers interest. But

are we prepared to allow employers to discriminate against employees because of their off the job habits? In addition, the organizations could be argued to have a moral duty to help their employees experiencing a substance abuse problem (just as they usually have a responsibility to provide health insurance coverage in order to help their employees with other, medical, problems) instead of just firing them. Again, an important aspect of this dilemma is the nature of the particular employment. In Skinner v. Railway Labor Executives' Association, Supreme Court of the United States held that the government's interest in ensuring the safety of the public justifies the rigorous testing regime employed by the defendant to monitor compliance with its sobriety politics. It is understandable how public interests attached to a particular profession might outweigh individual privacy concerns. But how can e.g. testing assembly line workers for marihuana be justified? First of all, there is no telling whether they engage in this activity exclusively in their own time, and, second, their job performance is usually effectively measured electronically and not projected by way of checking for sobriety. Arguably, employers would have no basis for testing in such cases, and yet, it is precisely low-level jobs like these one that seem to be at the centre of drug-testing efforts. One problem related to pre-employment testing, background checks and such procedures is their general unreliability and the related questions of whether the candidates in questions are given an adequate opportunity to verify and, if necessary, challenge this themselves. Finally, background checks might unintentionally reveal information of a deeply private character that may bear no relevance whatsoever to one's work potential.

On the job monitoring is the second key area of the disparity of moral interests in relation to the informational content about employees available to employers. **Electronic performance monitoring** is the key new element that amplified the concerns related to on the job surveillance. It makes all the traditional techniques easier, cheaper, faster and more comprehensive. It can make a difference between a traditional workplace and an equivalent of

a panopticon prison. As such, it radically transforms the situation for which principles of conduct in relation to employee monitoring have been traditionally negotiated and established.

However, not only surveillance techniques have been transformed by the rise of information technologies, but also, in some cases, the original motivation for surveillance. Employees sometimes spend much of their working time sending and receiving personal emails or surfing sites unrelated to their work. Arguably, electronic performance monitoring is the only way to counter such computer-based inappropriate workplace behaviour. One might be tempted at this time to put forward the argument that as long as the work is done, which sites an employee visits is none of employers business. And although this might make sense in many cases, selling such a line of reasoning when the employee in questions spends half of his or her time at work surfing sex sites might still be difficult.

The most common methods of electronic performance monitoring are keystroke loggers, packet monitors for examining network traffic (including e-mail and web activity monitoring) and electronic processing of video/audio data. **E-mail monitoring** has been particularly controversial because it has already led to a number of employees being fired. Separating private form business usage of email might be very difficult. Are we even sure what constitutes a private email? Just the fact of an email being sent from a private email portal would, arguably, still not be sufficient to qualify an email as private if the email is sent from a company's' computer and through a company's network, particularly if these are clearly announced to be exclusively for business purposes. But then, one might be pressed to do some private business, for example, receiving the results of medical testing, using such business-only network. Does that mean that the employer is entitled to this information? It is worth mentioning that the case law in the U.S. has regularly supported this notion that any communication going through the system owned by a company is in turn itself automatically

owned by that company. But are we comfortable with this reasoning? One counterargument often heard is that if two people are having a conversation in my house, a domain of my private property, we would still not consider that I am somehow entitled to the content of their conversation. Does the employment contract change that? As argued before, for many jobs it simply couldn't. If I am paid for my work and not for my not having private correspondence and private interests, than the economic interest of employers does not confer the right to monitor conversations, whether electronically or otherwise. One important factor, however, is an employer's interest in reducing liability exposure. Employers are expected to protect against sexual harassment and otherwise hostile environment, and some degree of monitoring might be necessary to do that. In fact, more than 20% of firms have been ordered by court to produce employee e-mail records.[4] In addition, in order to ensure the respect for software licensing laws, proprietary information and trade secrets, employers might simply have to monitor some aspects of computer usage in the workplace. For example, even if we concede that employers are not entitled to monitoring employees computer usage per se, the legal liability exposure for the possible pirated software installed on company's computers would confer some rights of insight to the employer.

Audio surveillance is another controversial area of employment monitoring. Audio surveillance is legal if the employer maintains the system (which is almost always the case) or the employee's consent for monitoring has been obtained. Again, the ethical argument is obviously different for the employees whose phone communication constitutes an essential part of their working contracts (e.g. help-desk agents and the like) and those who use phone communication only instrumentally, to perform a job the results of which are not confined to phone communication. **Video surveillance** is also increasing in popularity as a tool to monitor the workforce. The proponents argue that it discourages theft, physical

[4] Ibid. p. 2263

confrontations, and sexual harassment. Certainly, an organization can use video monitoring to reduce damaging actions by its employees and customers, thus potentially reducing its costs. However, video monitoring can rob employees of their privacy without a sufficient justification. Why should a company be allowed to video monitor employees if e.g. the potential loss due to theft is minimal? Most companies, however, are not required to produce such justifications. In addition to being potentially unnecessarily intruding, video surveillance has been a tool of major misuses, such as zooming in on body parts of customers and co-workers.

Finally, the most modern, advanced and powerful surveillance techniques seem to require even less human power and money to implement and operate. For example, time and labour (T&L) systems are now widely used to locate employees by tracking their magnetic badges, GPS capabilities of employees' cellular phones are used to track employees' locations (particularly the locations of the travelling salespeople), etc., enabling for major extensions to the traditional employee monitoring systems. These techniques of the future offer unprecedented surveillance possibilities and urge us to carefully weigh the interests of the parties involved.

Guidelines and Conclusions

In relation to the third level of critique presented in the second chapter, it is worth mentioning that the level of workplace surveillance differs around the world. However, these differences are primarily due to the diversity in technological capabilities and not necessarily ethical outlook. This, however, remains to be seen. Namely, the question of surveillance grew in importance only recently, and the legal response is in a nascent state, so the potential culturally based differences in reaction to this phenomenon cannot yet be observed. Western companies are performing the most far-reaching surveillance (which can be ascribed to technological differences) and still, European, Australian and New Zealand employees are

enjoying the most privacy protections. However, the realistic situation worldwide is that employees can expect little legal protection for their privacy in the modern workplace.

Legislation has traditionally been slow to address ethical issues arising from rapid technological advances. This is an important reason why one has to think about the principles applicable to the moral relations arising from employee surveillance. By analysing the interests of the parties involved, one can discern some general patterns. Employee surveillance has to balance the employer's interest in managing the workplace and the employees' privacy interest. The employer's right to manage the workplace is grounded in their economic interests as well as a number of other concerns, from workplace safety to intellectual property protection. Employees, on the other hand, deserve to be respected and treated as free and rational persons, capable of choosing for themselves how they live their lives. In finding a compromise between these two concerns, several key guiding principles can be used.

First, do no (unnecessary) harm. It is often possible to choose among different ways to organize workplace monitoring, and a thorough analysis of the situation coupled with an active empathy for the concerns of the employees can go a long way in helping determine which methods would be the least intrusive while still accomplishing the desired result. For example, a considerate attitude would be to examine employee's daily output only at the end of the day or at the end of the week instead of burdensome constant inspections. In fairness, many surveillance techniques, active personal oversight for one, serve only to provide employers with a sense of control, and not really to improve business performance. If an employee is slacking off, that will be just as evident at an end of a day (if it isn't, because the job is somehow done, than what is the problem?), and just the absence of a constant oversight might add to the overall workplace productivity. Therefore, the first principle that employers should bear in mind is the relation between the effectiveness and intrusiveness of monitoring.

In order for any method to be selected the employer should be able to demonstrate first that the goal of monitoring actually makes sense as well as that the incursions into employee privacy and wellbeing are minimal and unavoidable.

Second, following the analysis of the interests of the parties involved, it can be inferred that this demonstration of ethical permissibility of an employee surveillance method can only be carried out along three main lines of reasoning. The employer can show that intrusions into employee privacy are justified by his or her reasonable economic interests, that it is justified by the interests of the employee while proving that this policy would not present a case of illegitimate paternalism, or that it is justified as a means to protect a third party's (e.g. public's) legitimate interests.

Third, an important requirement in all instances of employee surveillance must be a respect for the employee privacy once the information is already gathered. Namely, many privacy incidents centred on the cases in which the information gathered for one of the three essential ethically permissible goals of employee surveillance was in fact used for different purposes. This rightfully creates a sense of betrayal on the part of the employee, and harms both the employee as well as the employer in the long run. In addition, a misuse of employee information is becoming increasingly dangerous. New technologies (e.g. genetic testing) now pose a serious threat to overall employee privacy and wellbeing if adequate measures to protect such information are not put in place.

Fourth, no surveillance whatsoever should take place absent informed consent of the employee. In addition, some room for dialogue must be left open. Unilaterally presenting an employee with a an information that he or she is going to be subject to surveillance is not fair, considering the power relations between the employer and the employee. The employee must be given a chance to participate in the discussion on the measures impacting such personal issues as privacy and workplace wellbeing.

Fifth, employees must be given the opportunity to avoid being monitored in at least some situations. Employees often need to conduct some personal business at the office and this does not mean that they should be made to share their personal life with the employer. For example, even if broad surveillance measures are justified, the employer could still set up a phone or a computer which is totally unmonitored in order to give employees an outlet for personal matters.

Sixth, in order to ensure workplace fairness, hierarchical equity of surveillance should be aspired to. Surveillance often depends on the employee's status within the organization, which can create a rift between those who are subject to surveillance and those who are not. In turn, this unequal treatment in such basic aspects as privacy could make the monitored workers feel like second-order employees.

Finally, an important aspect in relation to employee surveillance to bear in mind is trust. Niccolo Machiavelli suggested that between being feared and being loved by one's subordinates, one should always chose to be feared, as fear is easier to produce and easier to control. But the modern workplace is not about control, it is about people, creativity and trust. At the end of the day, the selection of workplace surveillance methods sends a message about how one perceives employees as persons and what kind of relationship with them one wants to nurture. As hard as it might be for many employers, it is often necessary to choose between tight control on the one side and trust, motivation and creativity on the other.

Case: Hewlett-Packard Spying Scandal

Hewlett-Packard is one of the largest computer companies in the world. It was founded in 1939 by Bill Hewlett and David Packard, then still students at Stanford. The first HP's product, a precision audio oscillator, was to become one of the many innovative products upon which HP build its rapid success. HP's corporate culture was imagined as family friendly, stable and conservative, with emphasis on high ethical standards in

conducting business activities. The fusion of radical innovation with high ethical standards eventually became known as “the HP way.”

Indeed, HP earned the respect of the world as an institution with admirable business ethics policies. It gradually became perceived as a standard-barrier of humanism and social responsibility in business. This unique reputation was consistently strengthened through responsible environmental policies, energy conservation, and most importantly, an unparalleled working environment that easily attracted the best and brightest. Arguably, the ability to recruit first-rate talent enabled HP to become a leader in the technology field. Top engineers, programmers and designers were readily joining HP, and key executives were easy to retain. HP’s managerial ranks were extremely open, and employees at all levels and across functions shared the vision of a successful and morally upright HP. The reputation for fairness and open-mindedness at HP was furthered in 1999, when Carly Fiorina became the CEO. She was the first woman ever to serve as CEO of a company included in Dow Jones Industrial Average. In February 2005, Fiorina was forced to resign and Patricia Dunn was promoted to chairwoman of the board. Having two women at the top of a Fortune 500 company was seen as a major victory in the fight against career glass ceiling for women, and HP was again praised as a paradigm of an ethically admirable and socially proactive company.

However, shortly after the resignation of Fiorina, it was becoming evident that confidential information in relation to HP’s long-term plans was being leaked to CNET Networks, Inc., a San Francisco media company. This was a serious problem because it undermined the shareholder information-sharing process and in turn fostered an atmosphere of mistrust within the company. HP’s need for information about the activities of its employees and the complexity of the related moral and legal issues were about to become a centre of a major controversy.

Patricia Dunn's response was to hire a private electronic-security company to find the source of the leaks to the media. In turn, those security experts recruited private investigators who started spying on reporters responsible for publishing the leaks as well as on a number of HP employees. The investigators used a method known as pretexting to obtain call records of HP board members and nine journalists, including reporters for the New York Times, the Wall Street Journal and CNET. Pretexting involved the investigators misrepresenting themselves as the board members and journalists in the process of obtaining information.

On September 11, 2006, CNET News.com released a letter by the U.S. House Committee on Energy and Commerce to Patricia Dunn in which she was informed of an investigation which discovered that "lies, fraud and deception" were used to acquire personal information on behalf of HP. They stated that they are "troubled" by this fact, "particularly that it involves HP—one of America's corporate icons." Dunn was summoned to testify before the Committee. She claimed she did not realize that pretexting involved identity misrepresentation and that she was absolutely sure that all the necessary information was obtainable legally.

Several other HP employees testified, including Kevin Hunsaker (former Senior Counsel and Director of Ethics and Standards of Business Conduct), Ann Baskins (former General Counsel) and Anthony Gentilucci (former chief of global investigations). They all invoked the Fifth Amendment, in effect refusing to answer questions of the Committee. Dunn resigned as chairwoman of HP's board, and Mark Hurd, the CEO, succeeded Dunn as chairman.

Criminal charges were filed and arrest warrants issued against these key actors. Four felony violations were alleged: conspiracy to commit crime, fraudulent use of wire, radio, or television transmissions, taking, copying, and using computer data and using personal

identifying information without authorization. The court decided that the charges would be dropped if the accused completed 96 hours of community service.

The case was quickly resolved and a lot of effort was put into restoring HP's reputation for ethical conduct. But, in order to appreciate the ethical dilemma Patricia Dunn faced, one must reflect on all the aspects of this situation. First, the leaks presented not just a major difficulty in relation to the shareholders, but also brought about a breakdown of trust within HP. The unknown employees leaking the information to the media were perceived as traitors of what has been established as a strong and proud HP corporate culture. Furthermore, the investigation, though unconventional, bore fruit. It was revealed that the actual source of the leaks were board members Gearge Keyworth and Thomas J. Perkins, both of whom were subsequently fired. In effect, Patricia Dunn succeeded in her quest to protect the information-sharing process. In addition, she did so without actually engaging in any illegal activity directly. The charges concentrated on the claim that she should have made an adequate effort to acquaint herself with the methods that were going to be used in the process of investigation. Was this element really under her control or were the investigators to respect the law regardless of HP's informational requirements?

No doubt that a wrong investigation company was hired, but questions linger as to whether any company at all should have been hired. Is it acceptable to spy on employees without their consent? What about when the stakes are as high as they were in the HP case? Which factors influence how we perceive this situation and does it merit a specific legal regulation?

Class Material

Conceptual Questions

- Who are the key ethical stakeholders in the matter of workplace surveillance?

- What are their respective interests?

- What is the role of employee consent in workplace monitoring?

- What is hierarchical equity of surveillance and why does it matter?

Critical Questions

- Are there limits to the surveillance of employees? What are they?

- Were there other less ethically challenging options open to Patricia Dunn and HP when faced with the leaks?

Further Readings

Books and Book Chapters

- Hartman, L. (2006). Technology and ethics: Privacy in the workplace. In K. W. Krasemann & P. H. Werhane (Eds.), Contemporary issues in business ethics. Lanham, MD: University Press of America.
- Lane, F. S. (2003). The naked employee: How technology is compromising workplace privacy. New York: AMACOM.
- Marcella, A. J., & Stucki, C. (2003). Privacy handbook: Guidelines, exposures, policy implementation, and international issues. New York: Wiley.
- Weckert, J. (Ed.). (2004). Electronic monitoring in the workplace: Controversies and solutions. Hershey, PA: Idea Group.

Journal Articles

- Halpern, D., Reville, P., & Grunewald, D. (2008). Management and Legal Issues Regarding Electronic Surveillance of Employees in the Workplace. Journal of Business Ethics, 80(2), 175-180.

- Hoffman, W. M., Hartman, L., & Rowe, M. (2003). You've got mail . . . and the boss knows. Business and Society Review, 108(3), 285–307.
- Martin, K., & Freeman, R. (2003). Some Problems with Employee Monitoring. Journal of Business Ethics, 43(4), 353-361.
- Persson, A., & Hansson, S. (2003). Privacy at Work: Ethical Criteria. Journal of Business Ethics, 42(1), 59-70.
- Whitman, J. Q. (2004). The Two Western Cultures of Privacy: Dignity versus Liberty. The Yale Law Journal, 113(6), 1151-1221.

Online Sources

- DeCew, J., 2006. Privacy. The Stanford Encyclopedia of Philosophy, Edward N. Zalta (ed.). [online] Available at: < http://plato.stanford.edu/entries/privacy/>